



----- KWIC -----

Abstract Text - FPAR (1):

PROBLEM TO BE SOLVED: To provide an information maintenance system that can easily restore user information for a mobile phone or a PHS when the mobile phone or the PHS is defective, lost or stolen or the model of the mobile phone or the PHS is changed.

Abstract Text - FPAR (2):

SOLUTION: Manual or automatic backup or mirroring of contents of a storage means 101 of a mobile phone 100 is applied to a storage medium 201 provided to a fixed storage device 200 such as a TV, a PC or a router. Backup or mirroring is applied to devices of backup or mirroring objects connected via a network after authentication between the devices with each other so as to prevent backups from taking place in order to avoid the backup or mirroring method from being illegally utilized.

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-112314

(P2002-112314A)

(43)公開日 平成14年4月12日(2002.4.12)

(51)IntCl <sup>7</sup>	識別記号	F I	キーワード(参考)
H 0 4 Q 7/34		G 0 6 F 3/06	3 0 4 F 5 B 0 1 7
G 0 6 F 3/06	3 0 4	12/14	3 2 0 A 5 B 0 1 8
12/14	3 2 0	12/16	3 1 0 M 5 B 0 6 5
12/16	3 1 0	H 0 4 B 17/00	R 5 K 0 2 7
H 0 4 B 17/00		H 0 4 M 1/00	V 5 K 0 3 3

審査請求 未請求 請求項の数 9 O L (全 10 頁) 最終頁に続く

(21)出願番号 特願2000-297454(P2000-297454)

(22)出願日 平成12年9月28日(2000.9.28)

(71)出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72)発明者 坂本 典哉

神奈川県横浜市磯子区新杉田町8番地 株

式会社東芝横浜事業所内

(74)代理人 100058479

弁理士 鈴江 武彦 (外6名)

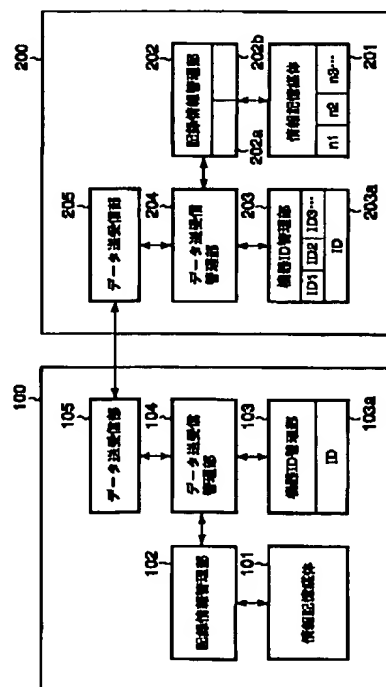
最終頁に続く

(54)【発明の名称】 情報保守システム及び情報保守方法

(57)【要約】

【課題】 携帯電話もしくはPHSが故障、紛失あるいは盗難されたとき、又は機種変更された場合に、ユーザの情報を容易に復元する。

【解決手段】 TV、PC、ルータ等の固定記憶装置200に設けられているストレージメディア201に、携帯電話100の記憶媒体101の内容を手動もしくは自動的にバックアップもしくはミラーリングをする。このバックアップ、ミラーリング手法が不正作業に利用できないように、ネットワークを接続してバックアップもしくはミラーリングする機器同士が互いに認証し合った後に、バックアップもしくはミラーリングの動作をすることで、複数のバックアップが行われることを防ぐ。



## 【特許請求の範囲】

【請求項1】外部機器と無線通信を行う第1の通信手段と、ユーザ情報を記憶する第1の記憶手段を有する携帯可能な携帯通信機器と、

前記携帯通信機器と通信を行う第2の通信手段、情報を記憶する第2の記憶手段、及び前記携帯通信機器と前記第2の通信手段を用いて通信を行い、前記第1の記憶手段に記憶されたユーザ情報を前記第2の記憶手段にバックアップするバックアップ制御手段を有し、所定位置に設置される固定記憶装置と、を具備することを特徴とする情報保守システム。

【請求項2】外部機器と無線通信を行う第1の通信手段と、ユーザ情報を記憶する第1の記憶手段を有する携帯可能な携帯通信機器と、

前記携帯通信機器と通信を行う第2の通信手段と、情報を記憶する第2の記憶手段、及び前記携帯通信機器の第1の記憶手段と前記第2の記憶手段とのミラーリングを行い、該ミラーリングの結果を前記第2の記憶手段に記憶するミラーリング制御手段とを有し、所定位置に設置される固定記憶装置と、を具備することを特徴とする情報保守システム。

【請求項3】前記携帯通信機器と前記固定記憶装置との無線LAN接続が可能であるかどうかを監視する監視手段と、前記無線LANの接続が可能となった時点で、該無線LANを介して自動的に前記バックアップもしくはミラーリングを開始する開始手段を更に具備することを特徴とする請求項1又は2記載の情報保守システム。

【請求項4】前記監視手段及び開始手段は共に前記固定記憶装置内に設けられることを特徴とする請求項3記載の情報保守システム。

【請求項5】前記監視手段及び開始手段は共に前記携帯通信機器内に設けられることを特徴とする請求項3記載の情報保守システム。

【請求項6】前記携帯通信機器は、前記第1の記憶手段における前記バックアップもしくはミラーリングする領域が予め設定されていることを特徴とする請求項1又は2記載の情報保守システム。

【請求項7】前記携帯通信機器を複数有し、前記固定記憶装置は前記第2の記憶手段内に各携帯通信機器に対応する複数の記憶領域を具備することを特徴とする請求項1又は2記載の情報保守システム。

【請求項8】外部機器と無線通信を行う第1の通信手段と、ユーザ情報を記憶する第1の記憶手段を有する携帯可能な携帯通信機器と、

前記携帯通信機器と通信を行う第2の通信手段、情報を記憶する第2の記憶手段、及び前記携帯通信機器と前記第2の通信手段を用いて通信を行い、前記第1の記憶手段に記憶されたユーザ情報を前記第2の記憶手段にバックアップするバックアップ制御手段を有し、所定位置に設置される固定記憶装置とを具備する情報保守システムに

おいて、

前記携帯通信機器が故障もしくは盗難に遭った時に、前記固定記憶装置の第2の記憶手段に記憶された前記携帯通信機器のユーザと信販会社との第1の契約情報を把握する工程と、

前記信販会社との通信により、前記携帯通信機器のユーザと該信販会社との第2の契約情報を把握する工程と、前記第1及び第2の契約情報が一致しているかどうかを確認する工程と、

10 該確認結果に応じて、前記固定記憶装置の第2の記憶手段に記憶された内容を、新たな携帯通信機器にダウンロードする工程、を具備することを特徴とする情報保守方法。

【請求項9】外部機器と無線通信を行う第1の通信手段と、ユーザ情報を記憶する第1の記憶手段を有する携帯可能な携帯通信機器と、

前記携帯通信機器と通信を行う第2の通信手段、情報を記憶する第2の記憶手段、及び前記携帯通信機器と通信を行い、前記第1の記憶手段に記憶されたユーザ情報を前記第2の記憶手段にバックアップするバックアップ制御手段を有し、所定位置に設置される固定記憶装置とを具備する情報保守システムにおいて、

前記携帯通信機器の機種変更時に、前記固定記憶装置の第2の記憶手段に記憶された前記携帯通信機器のユーザと信販会社との第1の契約情報を把握する工程と、前記携帯通信機器の前記第1の記憶手段に記憶されたユーザと前記信販会社との第2の契約情報を把握する工程と、

30 前記第1及び第2の契約情報が一致しているかどうかを確認する工程と、

該確認結果に応じて、前記固定記憶装置の第2の記憶手段に記憶された内容を、新たな携帯通信機器にダウンロードする工程、を具備することを特徴とする情報保守方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、ストレージメディアを利用して携帯電話又はPHSのメモリの内容をバックアップする方法に関する。

## 【0002】

【従来の技術】近年、映像・音声のデジタル信号処理技術がめざましく進歩し、それとともないアナログ放送信号をデジタル化した信号、もしくはデジタル放送信号がストレージメディアに記憶されるようになってきた。

【0003】主なストレージメディアとしては、大容量のものとしてはHDD、DVD RAMがあり、ブリッジメディアと呼ばれるSDカード、更にはパソコン等で使用されているフロッピー（登録商標）ディスク等がある。製品形態としては、TVもしくはセットトップボックス（STB）あるいはPCに上記ストレージメディア

を搭載するものが考えられる。

【0004】一方、携帯電話の普及はめざましく、製品形態も大容量メモリを搭載したものや、SIMカードや、SDカードを搭載可能なものも市場に投入されようとしている。携帯電話のメモリが大容量化するに伴い、個人情報等が大量に蓄積され、管理されるようになってきた。

【0005】

【発明が解決しようとする課題】今後、携帯電話はプリペイドカードあるいはクレジットカード等の機能を有するいわゆる電子財布となる可能性があることから、契約情報、チケット、クーポンなどの個人情報を盗まれないように管理する必要がある。そこで、携帯電話の機種変更もしくは携帯電話を盗難された場合などを考慮して、その内容をバックアップしておく必要がある。

【0006】しかし、現在その個人情報を自動的にバックアップする機能はなく、携帯電話が故障もしくは盗難に遭った場合に、蓄積されている情報が全て失われる可能性が高い。

【0007】従って本発明は、携帯電話もしくはPHSが故障、紛失あるいは盗難されたとき、又は機種変更された場合にユーザの情報を容易に復元することを目的とする。

【0008】又本発明は、上記の復元作業が不正作業に利用されることを防ぎユーザの損害を防止することを目的とする。

【0009】

【課題を解決するための手段】携帯電話もしくはPHSが故障、紛失あるいは盗難されたとき、又は機種変更された場合に備えて、TV、PC、ルータ等に設けられているストレージメディアに携帯電話もしくはPHSの記憶媒体の内容を手動もしくは自動的にバックアップもしくはミラーリングをする。

【0010】携帯電話もしくはPHSとTV、PC、ルータ等の固定記憶装置は、無線LAN等により無線チャンネルで接続される。携帯電話とTV、PC、ルータ等の固定記憶装置が確実に通信可能な距離まで近づくと、ネットワークが自動的に確立され、携帯電話の個人情報は自動的にバックアップ、もしくはミラーリングされる。

【0011】上記のバックアップ、ミラーリング手法が不正作業に利用できないように、ネットワークを接続してバックアップもしくはミラーリングする機器同士が互いに認証し、一度バックアップもしくはミラーリングを実施後は、機器同士が同じものである認証を行った後にバックアップもしくはミラーリングの動作をすることで、複数のバックアップが行われることを防ぐ。

【0012】更に、携帯電話が故障したとき、もしくは機種変更、あるいは紛失・盗難した場合には、携帯電話の契約会社に連絡して契約を破棄するとともに、旧携帯

電話の機体ID等の機器固有情報と、新たな契約を交わした新携帯電話の機体ID等の機器固有情報を一致させることで、上記TV、PC、ルータ等の固定記憶装置にバックアップ、ミラーリングされた情報を新たに契約した携帯電話へ情報のダウンロードすることを可能にする。

【0013】即ち本発明の情報保守システムは、外部機器と無線通信を行う第1の通信手段と、ユーザ情報を記憶する第1の記憶手段を有する携帯可能な携帯通信機器と、前記携帯通信機器と通信を行う第2の通信手段、情報を記憶する第2の記憶手段、及び前記携帯通信機器と前記第2の通信手段を用いて通信を行い、前記第1の記憶手段に記憶されたユーザ情報を前記第2の記憶手段にバックアップするバックアップ制御手段を有し、所定位置に設置する固定記憶装置とを具備する。

【0014】更に本発明の情報保守方法は、上記情報保守システムにおいて、前記携帯通信機器が故障もしくは盗難に遭った時に、前記固定記憶装置の第2の記憶手段に記憶された前記携帯通信機器のユーザと信販会社との第1の契約情報を把握する工程と、前記信販会社との通信により、前記携帯通信機器のユーザと該信販会社との第2の契約情報を把握する工程と、前記第1及び第2の契約情報が一致しているかどうかを確認する工程と、該確認結果に応じて、前記固定記憶装置の第2の記憶手段に記憶された内容を、新たな携帯通信機器にダウンロードする工程を具備する。

【0015】

【発明の実施の形態】以下、図面を参照しながら本発明の実施の形態について詳細に説明する。

【0016】先ず、携帯電話もしくはPHSと、TV、PCもしくはルータとの接続について図1を用いて示す。この実施形態では図1に示すように、携帯電話もしくはPHSと、TV、PCもしくはルータは無線LANにより接続される。TV、PCもしくはルータ200は所定位置に固定されているものとし、携帯電話もしくはPHS100が可搬なものとする（以下、携帯電話もしくはPHSを単に携帯電話、TV、PCもしくはルータを単に固定記憶装置という）。固定記憶装置200は例えば電話回線に接続され、様々な情報を送受信できる。

この無線LANの接続についてはA～Cの状態に大別できる。まず状態AはLAN領域外、状態BはLANボーダ領域、状態CはLANの接続できる領域である。

【0017】一般的に、LANには種類がいろいろあり、マスタースレーブの関係が固定のものと、どの機器もマスター／スレーブになれるLANがあるが、ここではどの機器もマスター／スレーブになれるものとして説明する。通常は電力の消費量を考えると、領域内にLANを接続できる機器が在るか否かは、上記固定記憶装置200がマスターとなって検知する事になる。しかし、場合によっては可搬できる携帯電話100のような機器

がマスターとなっても問題ない。

【0018】接続手順については、携帯電話100が有する記憶媒体の内容を固定記憶装置200の記憶媒体にバックアップする場合と、携帯電話100が有する記憶媒体の内容と固定記憶装置200の携帯電話に対応した記憶媒体の一部分とのミラーリングを実行する場合で若干異なる。

【0019】ここでミラーリングとは、携帯電話100と固定記憶装置200双方の記憶内容を全く一致させることで、この場合は携帯100の記憶情報の指定された一部、もしくは全体と固定記憶装置200の一部の内容が一致することになる。この場合、あらかじめ互いに登録されている携帯とHDD等の固定記憶装置200とのミラーリングを無線・有線で常に又は定期的に行う。例えば、Blue tooth-RS232Cを使ってPicoネットが構成できる範囲まで携帯電話100と固定記憶装置200が近づくと自動的にミラーリングをする。ミラーリングの範囲は予め設定される。具体的なものとしてHPのブックマーク等がある。更に、電話をかけることで、ミラーリングを行ってもよい。

【0020】又、バックアップとは、携帯電話100と固定記憶装置200双方の内容を一致させるのではなく、この場合は携帯100の情報の指定された一部、もしくは全体を固定記憶装置200に記憶することを意味し、携帯100の情報が新たな情報に入れ替わっても携帯100にかつて入っていた情報も固定記憶装置200側に残すことも可能である。この場合、あらかじめ互いに登録されている携帯と固定記憶装置200とのバックアップを無線・有線で常に又は定期的に行う。例えば、無線LANが構築され、該無線LANに確実に接続できる範囲まで携帯電話100とHDD等の固定記憶装置200が近づくと自動的に携帯電話からバックアップをする。

図2は本発明に係る携帯電話100及び固定記憶装置200の構成及び接続関係を示すブロック図であり、図3は本発明の第1の実施形態に係る動作として、携帯電話100の記憶情報を固定記憶装置200へバックアップする場合の通信状態遷移を示す。

【0021】この携帯電話100は、ユーザの個人情報を含む情報を記憶する情報記憶媒体101、情報記憶媒体101に対する情報の書き込み及び読み出しを管理する記憶情報管理部102、各携帯電話固有の機器ID103aを管理する機器ID管理部103、送受信される情報を暗号化及び復号化する機能を有するデータ送受信管理部104、携帯電話100に受信された信号を復調又は携帯電話100から送信される情報を変調するデータ送受信部105を有している。

【0022】固定記憶装置200は、携帯電話100の情報記憶媒体101に記憶されたユーザの個人情報を含む情報をバックアップするための情報記憶媒体201、

情報記憶媒体201に対する情報の書き込み及び読み出しを管理しバックアップ制御手段202aを有する記憶情報管理部102、この記憶装置200個々の機器ID203aを管理する機器ID管理部203、送受信される情報を暗号化及び復号化する機能を有するデータ送受信管理部104、この記憶装置200に受信された信号を復調又は記憶装置200から送信される情報を変調するデータ送受信部205を有している。尚、データ送受信205は携帯電話100が無線LAN領域内に在るか、つまり状態Cであるか否かを監視する監視手段205aを含む。

【0023】次に、バックアップする場合の通信状態手順を、上記固定記憶装置200がマスターになった場合を仮定して説明する。先ず図3のように、上記固定記憶装置200は無線LAN接続できる範囲に携帯電話100が入っているかどうかを監視手段205aにより随時監視することになる(ステップST1)。図1の携帯電話100が状態C(確実にLANが接続できることを確認できた状態)になったことを確認できた後、LAN接続機器認証の状態に入る(ステップST2)。この状態においては、図2に示す携帯電話100と固定記憶装置200のそれぞれの機器ID管理部103及び203に管理されているID103a及びID203aを元にお互いに認証が行われる。相互のIDの確認が完了し、IDが認められた場合にのみ、LANの接続が行われる。

【0024】その後、このバックアップ動作の場合、図3に示すように携帯電話100側からバックアップ要求が出され、バックアップする事が許されるかどうかの機器認証が更に行われる(ステップST4)。このとき、ステップST2におけるLANを接続できるかどうかの認証と同じIDが使われる可能性があるが、バックアップ許可は不正アクセスによって複製が多くできてしまう可能性を秘めているので、この認証動作は非常に厳格に行う必要がある。従って、図2に示す機器ID管理部103からデータ送受信管理部104を介して出力されるID103aは、ステップST4においては平文ではなく暗号化されていてもよい。

【0025】従って、携帯電話100及び固定記憶装置200のID情報は、鍵情報と共にデータ送受信管理部104によって暗号化又は復号化され、データ送受信部205を介して送受信されて認証が行われる。TV等の固定記憶装置200側においても、同様の処理が行われる。このとき、認証が正常に完了しない場合、つまりどちらかの機器の信頼性が疑わしい場合は、バックアップを中止し、その情報をユーザに提供する。

【0026】機器の認証が正常に完了した後に、バックアップ動作開始の指示がバックアップ制御手段202aに出され、バックアップが行われる(ステップST5)。バックアップ動作完了後にバックアップ完了通知がマスター側である固定記憶装置200から携帯電話1

00に送られる(ステップST6)。

【0027】LANが接続されている状態においては、携帯電話100の記憶媒体101の内容が更新されると、バックアップ開始要求がステップST3のように出され、以降は上記説明した動作が繰り返される。

【0028】また、バックアップ動作中にLANの接続が切れるような事があった場合は、図2の記憶情報管理部102、202においてその状態を保持し、再度LAN接続が行われた場合に、その情報を元にバックアップを再開するか、もしくは状況に応じて全く初めから動作を繰り返す。尚、このバックアップされる内容には、インターネットのURL等が含まれる。

【0029】次に、携帯電話の記憶媒体101の内容とTV等の固定記憶装置200の携帯電話に対応した記憶媒体201の一部分をミラーリングする動作を本発明の第2の実施形態として説明する。図4はこのミラーリングする場合の通信状態遷移を示す。

【0030】LAN接続する状況は、図3のバックアップの場合と変わらない(ステップST11及びST12)。その後、図4に示すようにミラーリング要求が、マスターがTV等の固定記憶装置200の場合に、固定記憶装置200側から携帯電話100に送られ(ステップST15)、ミラーリングする事が許されるかどうかの機器認証が行われる(ステップS14)。又、携帯電話100側がマスターの場合は携帯電話100からミラーリング要求が出され、ミラーリングする事が許されるかどうかの機器認証が行われる。

【0031】このとき、上記LANを接続できるかどうかの認証と同じIDが使われる可能性があるが、バックアップ許可と同様に不正アクセスによって複製が多くできてしまう可能性を秘めているので、認証の動作は非常に厳格に行う必要がある。従って、図2に示す機器ID管理部103からデータ送受信管理部104を介して出力されるID103aは、ステップST14においては平文ではなく暗号化されていてもよい。

【0032】従って、携帯電話100及び固定記憶装置200のID情報は前述したように、鍵情報と共にデータ送受信管理部104によって暗号化又は復号化され、データ送受信部205を介して送受信されて認証が行われる。TV等の固定記憶装置200側においても、同様の処理が行われる。このとき、認証が正常に完了しない場合、つまりどちらかの機器の信憑性が疑わしい場合は、ミラーリングを中止し、その情報をユーザに提供する。

【0033】機器の認証が正常に完了した後に、ミラーリング動作開始の指示がミラーリング制御手段202bに出され、ミラーリング動作が行われ(ステップS15)、動作完了後にミラーリング完了通知が、マスター側が固定記憶装置200の場合には固定記憶装置200から携帯電話100に送られる(ステップS16)。こ

のとき、ミラーリング動作は、携帯電話100側の情報が最新であれば、携帯電話100側の情報が固定記憶装置200側に情報が送られ、逆に固定記憶装置200側の情報が最新であれば、固定記憶装置200側から携帯電話100側に情報が送られ記憶されることになる。マスターが携帯電話側の場合は、携帯電話100からミラーリング完了通知が固定記憶装置200に送られる。

【0034】LANが接続されている状態においては、携帯電話100の記憶媒体101の内容もしくは固定記憶装置200の携帯電話に対応する記憶媒体201の一部分が更新されると、ミラーリング開始要求が出され、以降は上記説明した動作が繰り返される。

【0035】ここで、ミラーリングされるべき内容は、事前にユーザが設定できるようにする事も可能である。また、ミラーリング動作中にLANの接続が切れるような事があった場合は、図2の記憶情報管理部102、202においてその状態を保持し、再度LAN接続が行われた場合に、その情報を元にバックアップを再開するか、もしくは状況に応じて全く初めから動作を繰り返す。

【0036】本発明の第3の実施形態として、TV等の固定記憶装置200側と携帯電話100側がケーブル等により1対1で繋がるような場合は、図3、図4におけるステップST1及びST11のようなLAN接続手順を省くことが可能で、以下の動作は第1及び第2の実施形態と同様に行うことでバックアップ、ミラーリングが可能となる。

【0037】本発明の第4の実施形態として、1台の固定記憶装置200を複数のユーザが使用する場合、固定記憶装置200の機器ID管理部203には、固定記憶装置200自身のID203aの他に、図2のように複数のユーザが使用している携帯電話のID1、ID2、ID3…が格納され、更に情報記憶媒体201の携帯対応部分が、M1、M2、M3…のように複数設けられる。固定記憶装置200はこれら複数のID1、ID2…を参照して通信相手から送られてくる機器IDを認証してからバックアップ又はミラーリングを行う。

【0038】次に本発明による第5の実施形態を説明する。携帯電話が紛失あるいは盗難等によって使用不可能になった場合、又は機種変更する場合は、携帯電話の契約の抹消をし、その後契約を新たに行う。この第5の実施形態の場合、今までの携帯に蓄積されていた情報を速やかに固定記憶装置からダウンロードすることを可能とする。このとき、固定記憶装置側からダウンロードを許可できる携帯かどうかを認識する必要がある。

【0039】図5は第5の実施形態に係る可搬機器としての携帯電話110及びTV等の固定記憶装置210の構成及び接続関係を示すブロック図、図6は携帯電話110が故障もしくは盗難に遭った場合及び機種変更する場合の処理を示すフローチャートである。

【0040】図5に示すように、この第5の実施形態に係る携帯電話110の基本的構成は図2の携帯電話100と同様であるが、情報記憶媒体111がユーザ管理領域111a及び信販会社管理領域111bを有する点が異なる。この信販会社管理領域111bには信販会社へのユーザ登録番号や電子マネー情報等の信販会社が管理する情報が記憶される。ユーザ管理領域111aにはこの信販会社が管理する情報以外のユーザ個人情報が記憶される。

【0041】又、本実施形態に係る固定記憶装置210の基本的構成は図2の固定記憶装置200と同様であるが、情報記憶媒体211が携帯電話110の情報記憶媒体111に対応してユーザ管理領域211a及び信販会社管理領域211bを有し、更にモデムもしくは移動体通信モジュール218が設けられる点異なる。このモデムもしくは移動体通信モジュール218により、固定記憶媒体210は電話網300を介した通信が可能となる。

【0042】先ず、携帯電話110が故障、もしくは盗難に遭った場合は、ユーザが携帯電話会社において故障または盗難の届け出をする。そして、図6(a)のステップST21のように携帯電話会社が、故障もしくは盗難にあった携帯電話の情報をバックアップしている固定記憶装置210の信販会社管理領域211bに、電話網もしくは移動体通信網300及びモデムもしくは移動体通信モジュール218を介してアクセスし、信販会社管理領域211bのバックアップした時間及び内容を確認する。

【0043】次に携帯電話会社はステップST22のように、信販会社（携帯電話の電子マネーや電子チケットを管理している会社）に、故障もしくは盗難にあった携帯電話110の登録の内容（登録番号等）を確認する。そしてステップST23のように、ステップST21で確認した信販会社管理領域211bの内容及びバックアップした時間と、ステップST22で信販会社に問い合わせた内容が一致しているかどうか確認する。

【0044】ステップST23で一致している場合は、故障もしくは盗難にあった携帯電話110の登録内容を新しい携帯電話に、固定記憶装置210の記憶媒体211からダウンロードすることを許可するためのIDを付与する（ステップST24）。このIDは一般に故障もしくは盗難に遭った携帯電話で使用されていたIDである。ステップST23で一致していない場合は、故障もしくは盗難に遭った携帯電話110の登録内容を新しい携帯電話に固定記憶装置210の記憶媒体211からダウンロードすることを許可しないか、もしくは一部分のみ許可するためのIDを付与する（ステップST25）。例えば、信販会社へのユーザ登録番号のみが一致し、電子マネー情報が一致しない場合、電子マネー情報を除く他の情報のダウンロードを許可するためのIDが

機種変更後の新しい携帯電話に付与される。。

【0045】次にユーザが携帯電話110の機種を変更する場合の処理を図6(b)を参照して説明する。

【0046】携帯電話110の機種を更新する場合は、ユーザが携帯電話会社において機種更新の届け出をする。そして、ステップST31のように携帯電話会社が、古い携帯電話の情報をバックアップしている固定記憶装置210に設けられた信販会社管理領域211bに、電話網もしくは移動体通信網300及びモデムもしくは移動体通信モジュール408を使ってアクセスし、信販会社管理領域211bのバックアップした時間及び内容を確認する。

【0047】次に携帯電話会社は古い携帯電話110の信販会社管理領域111bの内容及びバックアップした時間を確認する。そしてステップST32のように、この古い携帯電話210の信販会社管理領域111bの内容及びバックアップした時間と、ステップST31で確認した固定記憶装置210の信販会社管理領域211bの内容及びバックアップした時間が一致しているかどうか確認する。

【0048】一致している場合はステップST32のように、機種変更した新しい携帯電話に、固定記憶装置210の記憶媒体211からダウンロードすることを許可するためのIDを付与する。一致していない場合はステップST33のように、機種変更した新しい携帯電話にTV等の固定機器の記憶媒体からダウンロードすることを許可しないか、もしくは一部分のみ許可するためのIDを付与する。例えば、信販会社へのユーザ登録番号のみが一致し、電子マネー情報が一致しない場合、電子マネー情報を除く他の情報のダウンロードを許可するためのIDが機種変更後の新しい携帯電話に付与される。情報記憶媒体111aのユーザ管理領域302については、ユーザが管理している個人情報なので、信販会社へのユーザ登録番号が一致していれば固定記憶装置210のユーザ管理領域211aのバックアップ、ミラーリングは自由である。

【0049】

【発明の効果】以上説明したように本発明によれば、携帯電話もしくはPHSが故障したとき、又は機種変更あるいは紛失・盗難した場合に、ユーザの情報を新しい機器に容易に復元することが可能となる。又本発明によれば、バックアップ、ミラーリング手法が電子マネーの複製等の不正作業に利用できないようにすることが可能となる。

【図面の簡単な説明】

【図1】TV等の固定機器と携帯電話もしくはPHS等の可搬機器の無線LAN接続状態を示す構成図。

【図2】TV等の固定機器と携帯電話もしくはPHS等の可搬機器のシステム構成図。

【図3】TV等の固定機器と携帯電話に、PHS等の可



搬機器の情報をバックアップする時の接続手順図。

【図4】TV等の固定機器と携帯電話に、PHS等の可搬機器の情報をミラーリングする時の接続手順図。

【図5】TV等の固定機器と携帯電話もしくはPHS等の可搬機器の他のシステム構成図。

【図6】携帯電話が故障もしくは盗難に遭った場合及び機種変更する場合の処理を示すフローチャート。

【符号の説明】

100、110…携帯電話

101、111、201、211…情報記憶媒体

102、114、202、214…記録情報管理部

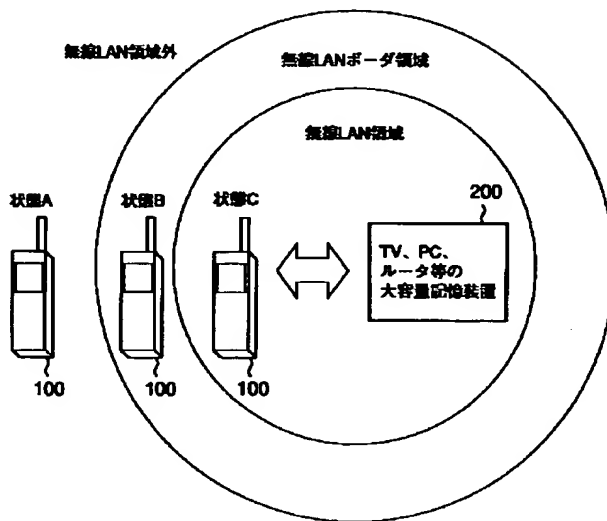
103、115、203、215…機器ID管理部

104、116、204、216…データ送受信管理部

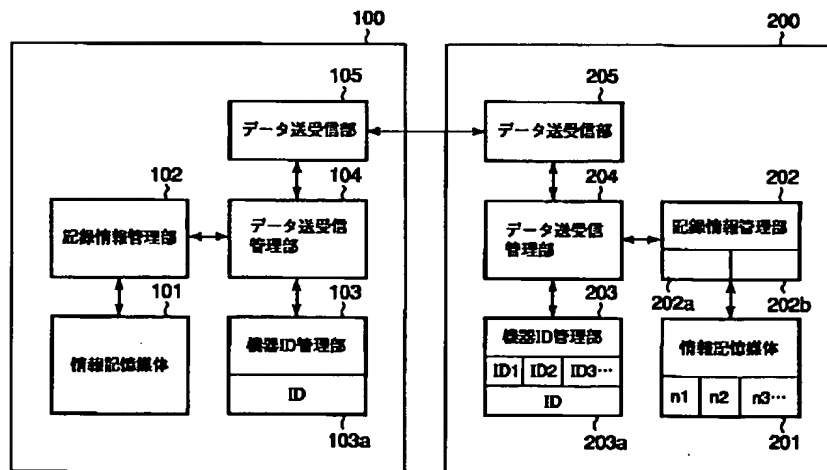
105、117、205、217…データ送受信部

200、210…固定記憶装置

【図1】



【図2】



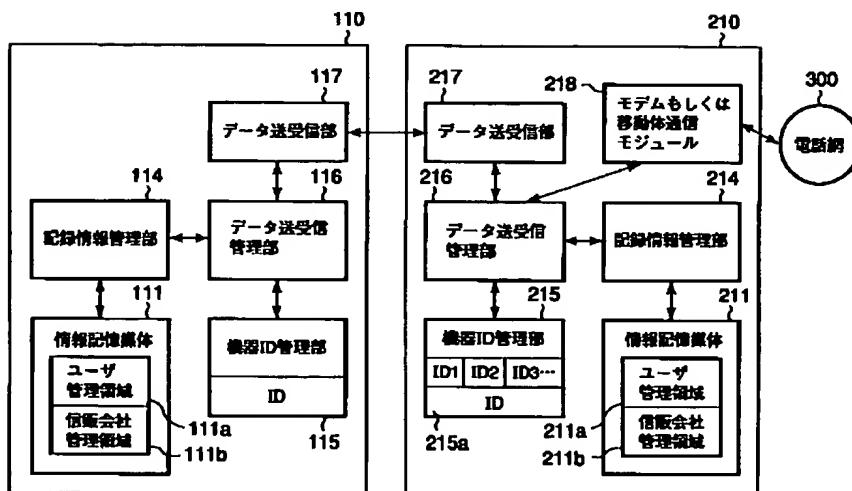
【図3】



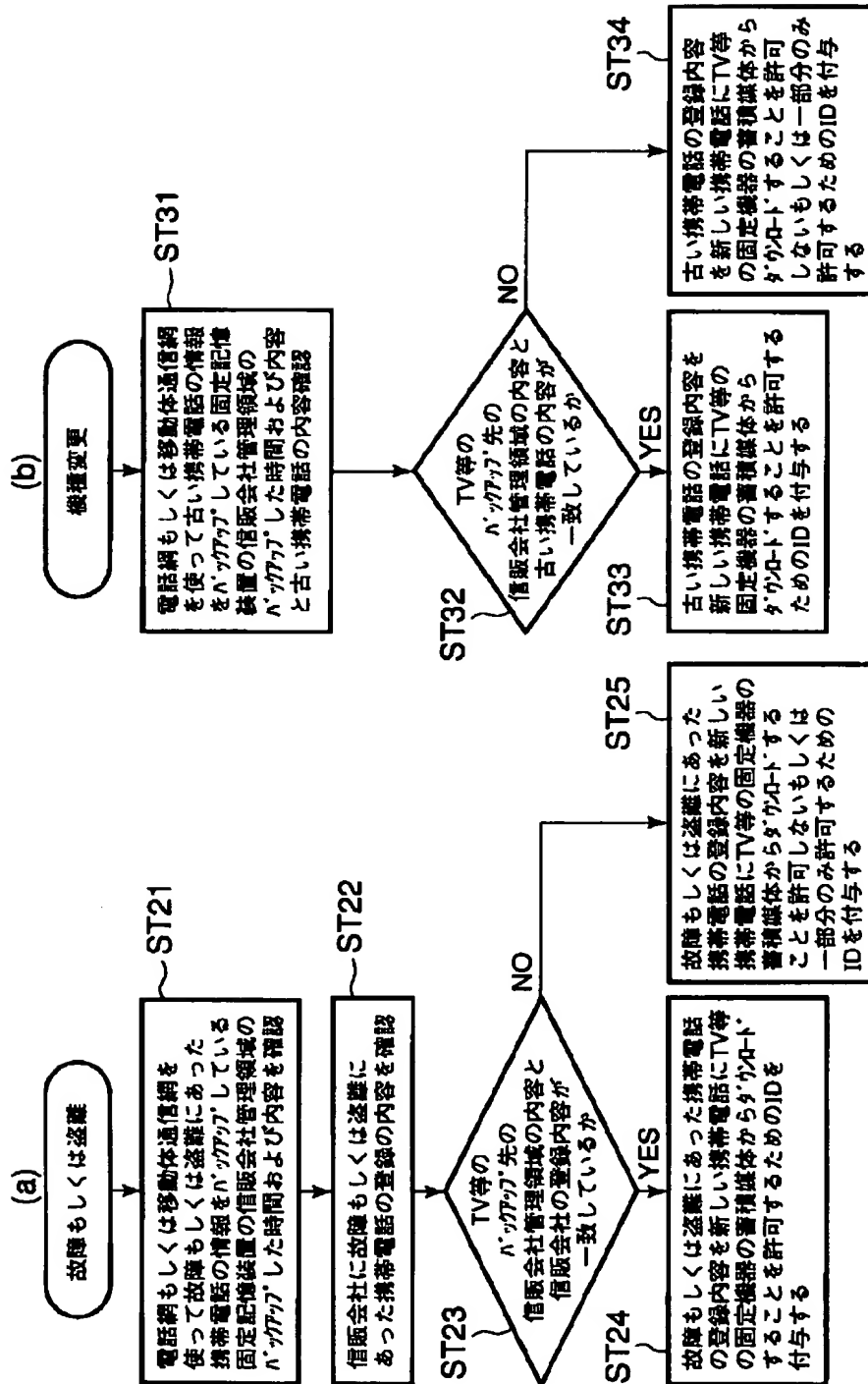
【図4】



【図5】



【図6】



## フロントページの続き

(51)Int. Cl. <sup>7</sup>	識別記号	F I	タームコード' (参考)
H 0 4 L 12/28		H 0 4 M 1/727	5 K 0 4 2
H 0 4 M 1/00		H 0 4 Q 7/04	B 5 K 0 6 7
1/727		H 0 4 L 11/00	3 1 0 B

Fターム(参考) 5B017 AA03 AA07 BA06 BB09  
 5B018 GA04 HA02 HA03 HA04 HA05  
 KA03 KA22  
 5B065 BA01 CC08 CE23 EA33 PA15  
 5K027 AA11 BB01 CC08 HH26  
 5K033 AA06 DA19 DB12  
 5K042 AA01 AA06 CA13 DA32 EA14  
 FA11 FA15 JA01 JA08  
 5K067 AA26 AA32 DD17 EE02 EE16  
 GG01 HH23 HH24 KK15 LL05